IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH DJRPUNKROCKPRINTER@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, INC., MOUNTAIN VIEW, CA	Case No. 7:20mj70 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jerre E. Harvard III, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account, **DJRPUNKROCKPRINTER@GMAIL.COM,** that is stored at premises controlled by Google, Inc., an email provider headquartered at Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Gmail to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (HSI) since March, 2008 and am currently assigned to HSI-Washington, DC, Roanoke, Virginia field office. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child

exploitation, and child pornography. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in Title 18, United States Code, Section 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including Title 18, United States Code, Section 2252, and I am authorized by law to request a search warrant.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2252(a)(2) and (b)(1) (distribution of a visual depiction of a minor engaged in sexually explicit conduct) have been committed by unknown persons. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The Kik application is designed for mobile chatting or messaging. To use this application, a user downloads the application to a mobile phone or other mobile device via a service such as Google Play Store, Apple iTunes, or another similar provider. Once downloaded

and installed, the user is prompted to create an account and username. The user also has a display name, which is what other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature, and the two parties can then send each other messages, images, and/or videos.

7. Kik users are also able to create chat groups, of up to 50 people, to communicate in a group setting and exchange images and/or videos. These groups are administered by the group creator who has the authority to remove and/or ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a "hashtag" that is easily identifiable or searchable by keyword.

8. In approximately August, 2019, the Kik messaging application provided information to law enforcement that a Kik user with the username "reveredoni," email address **djrpunkrockprinter@gmail.com**, and account name Demon Tetsuko had posted child abuse material to the Kik messaging platform.

9. The abuse material accompanying the lead from Kik was a 7 second video depicting what appeared to be a topless 10-14yo female massaging her left breast.

10. Your affiant has been advised by an HSI forensic analyst this abuse material file was created on August 9, 2019 at 04:04:12 UTC, exactly one second before it was uploaded to Kik at 04:04:13 UTC. The audio sample rate is set at 44.1, which is consistent with certain iPhone models. This metadata/EXIFdata suggests that the video was created natively on Kik and uploaded immediately afterwards, possibly from an iPhone.

11. Snapchat is a multi-media messaging application with a primary function of person-to-person photo sharing with a feature that causes the photo to self-delete after a period of

time (deletion time determined by the sender). Users can send "snaps" including photos or videos, chats including message communications, or save data in a "memories" file. Certain degrees of user anonymity, enhanced application messaging security and the photo-deletion features have made Snapchat a popular mode of communication for persons sending sexually explicit images. Snapchat has a procedure for maintaining account information and content that is the subject of complaints related to inappropriate or illicit behavior.

12. In or about May, 2020, the National Center for Missing and Exploited Children (NCMEC) provided information to law enforcement regarding a Snapchat user with the screen name "drpunkrockso," email address **djrpunkrockprinter@gmail.com**, and date of birth July 13, 1985. The NCMEC information regarding this Snapchat user also included an IP address connection from 2601:5c9:100:3741:14f7:1e5d:9810:8d66 occurring on or about October 17, 2019 08:40:07 UTC. The IP address is provided by Comcast and from the Pulaski, Virginia 24301 area.

13. Three still images posted to Snapchat accompanied this lead. Two images appeared to be the same. This image depicts a suspected minor female engaging in vaginal sex with an adult male. The adult male appears to have ejaculated. No other body parts are visible on the female except for the groin area.

14. The third image depicts a possible 7-9 year old minor female exposing her vagina and breasts and an adult wearing a costume mask performing oral sex on the minor female.

15. An internet search of "drpunkrockso" revealed a Facebook account with username Jon-Michael Lynch. A further review of the Facebook page revealed that Jon-Michael Lynch lives in Draper, Virginia and is in a relationship with a female identified as C. K.

16. Draper, Virginia is in Pulaski County, Virginia, which is in the Western District of Virginia.

17. The National Law Enforcement Telecommunications System (NLETS) was queried with the name Jon-Michael Lynch and date of birth provided from Snapchat of July 13, 1985. NLETS returned that a Jon-Michael Ryan Lynch with date of birth July 13, 1985 resides at 4076 Kirby Rd, Draper, Virginia 24324. Jon-Michael Ryan Lynch is described as a white male, 5'11", 130 pounds. A query of the National Crime Information Center (NCIC) revealed that Jon-Michael Lynch has no criminal history.

18. A Facebook post made to the account of Jon-Michael Lynch on July 14, 2019 revealed the text "Thanks for the awesome birthday wishes everyone!!!!" In your affiant's training and experience, it is common that users of social media will post a birthday thank you message contemporaneously to their actual birthday.

19. In general, an email that is sent to a Gmail subscriber is stored in the subscriber's "mail box" on Gmail servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Gmail servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Gmail's servers for a certain period of time.

20. Therefore, there is probable cause to believe that the contents the Gmail account **DJRPUNKROCKPRINTER@GMAIL.COM** with contain confirmatory emails from both Kik and Shapchat and information related to those platforms services. It is likely that information showing that the user of this Gmail account is also the user of each of the Kik and Snapchat accounts above has been preserved on Gmail's servers. From my training and experience, information about the identity of the user of these accounts is also likely to be contained in the information requested by the search warrant.

BACKGROUND CONCERNING EMAIL

21. In my training and experience, I have learned that Gmail provides a variety of on-line services, including electronic mail ("email") access, to the public. Gmail allows subscribers to obtain email accounts at the domain name gmail.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Gmail. During the registration process, Gmail asks subscribers to provide basic personal information. Therefore, the computers of Gmail are likely to contain stored electronic communications (including retrieved and unretrieved email for Gmail subscribers) and information concerning subscribers and their use of Gmail services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

22. A Gmail subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Gmail. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, on-line cloud storage, email in the account, and attachments to emails, including pictures and files.

23. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such

information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

24. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

25. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

26. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

27. Based on the forgoing, I request that the Court issue the proposed search warrant.

28. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Gmail. Because the warrant will be served on Gmail, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

JERRE E HARVARD III

Digitally signed by JERRE E HARVARD III
Date: 2020.06.10 08:02:12 -04'00'

Jerre E. Harvard III
Special Agent
Department of Homeland Security
Homeland Security Investigations

Subscribed and sworn to before me on June 10, 2020

Robert S. Ballou

Honorable Robert S. Ballou
UNITED STATES MAGISTRATE JUDGE